

FILED**UNITED STATES DISTRICT COURT
ALBUQUERQUE, NEW MEXICO****UNITED STATES DISTRICT COURT****AUG 22 2016**for the
District of New Mexico**MATTHEW J. DYKMAN
CLERK**In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

See Attachment A.

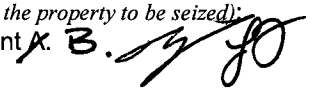
Case No.

16mr 594

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

located in the _____ State and _____ District of _____ New Mexico _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment A. B. 

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. 1029

18 U.S.C. 1028

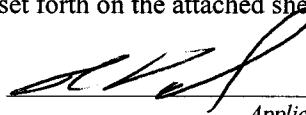
Offense Description

Fraud and related activity in connection with access devices.

Fraud and related activity in connection with identity documents.

The application is based on these facts:
See attached Affidavit, Attachment A, and Attachment B, incorporated herein by reference.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Ryan Palmiter, HSI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 8/22/2016City and state: Albuquerque, New Mexico



Judge's signature

Laura Fashing US Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO**

**IN THE MATTER OF THE
APPLICATION FOR AN ORDER
AUTHORIZING THE SEARCH
OF;** Apple iPhone model A1586
with International Mobile Equipment
Identity (IMEI) 356954068692712,
and a Toshiba Satellite computer
with serial number 1D227418Q.

Magistrate No.

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

1. I, Special Agent Ryan Palmiter, am currently employed with Immigration and Customs Enforcement, U.S. Department of Homeland Security, Homeland Security Investigations (HSI), in Albuquerque, New Mexico. I have been employed with HSI since February 18, 2011. Prior to employment with HSI, I was employed as an Immigration Enforcement Agent, with Immigration and Customs Enforcement in 2008. I am currently assigned to the General Crimes Investigations group in Albuquerque, where I conduct investigations including but not limited to violations related to Identity/Benefit Fraud and Identity Theft. I have conducted numerous investigations involving Identify Theft and Fraud as well as prepared and executed several search and seizure warrants.

ITEMS TO BE SEARCHED

2. This affidavit is submitted in conjunction with an application for authorization to forensically search:
A) Apple iPhone model A1586 with International Mobile Equipment Identity (IMEI) 356954068692712
B) Toshiba Satellite computer with serial number 1D227418Q.
3. This affidavit is based upon information I have gained from my investigation, my personal observations, training and experience, as well as upon information related to me by other individuals, including law enforcement officers. In making this affidavit, I am relying on information from my own personal observations and in part on information received from Detective Jimmy Jones of the Albuquerque Police Department (APD).

Your affiant believes there is probable cause and respectfully requests an order authorizing the search of the electronics described in paragraph 2 and further described in Attachment A.

4. Since this affidavit is being submitted for the limited purpose of securing a search and seizure warrant, I have not included each and every fact known to me concerning this investigation but have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence relating to violations of 18 U.S. Code § 1029, Fraud and Related Activity in Connection with Access Devices and 18 U.S. Code § 1028, Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information, will be located within the items described in attachment A.

BACKGROUND

5. On March 3, 2016, at approximately 1000 hours, NMSP Officer Aguirre contacted the U.S. Department of Homeland Security, Homeland Security Investigations (HSI) for assistance. NMSP Officer Aguirre requested assistance in order to further investigate what he believed to be suspicious items inside the Subject Vehicle. Officer Aguirre relayed to HSI Special Agents Palmiter and Allen that he initiated a traffic stop on the Subject Vehicle for a traffic violation of Following Too Closely. The traffic stop was conducted on Interstate 40 eastbound at approximately mile marker 140. Encountered in the vehicle were the driver, Daryl Sandoval and one passenger, Monica Acosta.
6. Officer Aguirre relayed to HSI Special Agents that he observed a rental agreement for the vehicle which listed Acosta as the renter and only authorized driver. Registration information indicated the Subject Vehicle was registered to EAN Holdings LLC doing business as Enterprise-Rent-A-Car. Officer Aguirre informed HSI Special Agents that Sandoval did not possess a valid driver's license, only an identification card, and was not listed as an authorized driver on the rental agreement.
7. Officer Aguirre performed a consent search of the vehicle and upon opening a compartment located behind the passenger seat and below the floorboard of the vehicle (This is a factory storage compartment referred to by the manufacturer as a "stow and go") discovered a credit card embosser, a credit card encoder/decoder, two grocery style shopping bags containing numerous prepaid credit/debit cards, and a fingernail file/buffer.
8. Through the open passenger side sliding van door, HSI Special Agents Palmiter and Allen could see in plain view the items Officer Aguirre described; a credit/debit card embosser, a credit/debit card encoder/decoder, two bags with numerous prepaid cards, as well as the fingernail buffer. Your Affiant knows through training and experience that these items are commonly used to deface, alter, and convert common access cards in order to produce replicas of legitimate credit and debit cards. Special Agents Palmiter and Allen asked Sandoval if he was willing to speak to them but he declined. Sandoval also declined permission for Special Agents Palmiter and Allen to search the van.
9. The Subject Vehicle was photographed, sealed, and towed to the HSI office.

10. On March 7, 2016, a federal search and seizure warrant was issued for the Subject Vehicle by a United States Magistrate Judge. HSI Special Agents executed the search warrant on the same date and recovered multiple stored value cards, a credit card decoder/encoder terminal, a credit card embossing machine, a point of sales terminal, a credit card stamping machine and several finger nail buffers. These items were found in the Subject Vehicle's Stow and Go compartment located behind the front passenger seat.
11. A separate federal search warrant was issued on March 15, 2016 for the electronic devices found in the vehicle.
12. On March 10, 2016, Special Agent Palmiter was contacted by Albuquerque Police Detective (APD) Jimmy Jones concerning a victim whose credit card information was stolen and used in Albuquerque. Detective Jones went to the business, where the stolen credit card information was used. Detective Jones spoke to the store manager. The store manager was able to identify Monica Acosta as the person who used the credit card in questions. Acosta provided the store with a Nevada driver's license as proof of identity.
13. On March 11, APD located Acosta and Sandoval and conducted a traffic stop on their vehicle. APD seized the vehicle and obtained a search warrant for the vehicle.
14. Found during the search warrant were several stored value cards with the name Monica Acosta affixed with a label. A stored value card is a payment card with a monetary value stored on the card itself, not in an external account maintained by a financial institution. In addition to the stored value cards, APD also located a label maker, a magnetic card reader/encoder, several stored value card blanks, an Apple iPhone model A1586 with International Mobile Equipment Identity (IMEI) 356954068692712, and a Toshiba Satellite computer with serial number 1D227418Q. *These items have remained in APD custody since March 11, 2016. AS LJ*
15. Persons engaged in criminal activity involving stored value cards often use a "reader writer encoder" machine which allows them to remove any existing information stored on the magnetic stripe and replace it with stolen/compromised information. This information can include the credit account number and "track data" from an unsuspecting victim. Track Data is described as the categories of information encoded on the magnetic stripe of a credit card. In addition, an encoder machine can also place a victim's bank account information on the magnetic stripe. This allows the criminal to use a stored value card to purchase high end merchandise easily sellable on the black market while draining the funds of an unsuspecting victim's bank account.
16. Your affiant knows through his training, knowledge, and experiences that computers and electronic media are used to receive and store stolen/compromised credit card information. Also, a computer or item of similar capabilities is needed to operate the credit card decoder/encoder found during the search.
17. Your affiant has probable cause to believe that records, evidence, fruits and instrumentalities relating to violations of 18 U.S. Code § 1029, Fraud and Related

Activity in Connection with Access Devices and 18 U.S. Code § 1028, Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information are held within the Apple iPhone model A1586 with International Mobile Equipment Identity (IMEI) 356954068692712, and the Toshiba Satellite computer with serial number 1D227418Q.

SEARCH AND SEIZURE

CELLULAR PHONES, COMPUTERS AND ELECTRONIC STORAGE

1. As described above and in Attachment B, this application seeks permission to search for and seize records believed to exist on Apple iPhone model A1586 with International Mobile Equipment Identity (IMEI) 356954068692712, and a Toshiba Satellite computer with serial number 1D227418Q, described more particularly in Attachment "A", in

whatever form they are found. Upon discovery of records relating to the listed violation, this application seeks permission to include Apple iPhone model A1586 with International Mobile Equipment Identity (IMEI) 356954068692712 is identified as a smartphone by its manufacturer. Your Affiant knows from training and experience that smartphones have many of the same capabilities and operating system as a computer and has access to the internet, including web browsers, e-mail programs, and chat programs. One form in which the records might be found is data stored on a computer's hard drive or other storage media to include external storage media connected to the cellular device. Thus, the warrant applied for would authorize the seizure of electronic storage media and the copying of electronically stored information, all under Rule 41(e) (2) (B).

2. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crime described in this warrant, but also for forensic electronic evidence that establishes how computers or other electronic devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the Apple iPhone model A1586 with International Mobile Equipment Identity (IMEI) 356954068692712, and a Toshiba Satellite computer with serial number 1D227418Q because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of external storage media, and the times the smartphone was in use. Smartphone file systems can record information about the dates files created and the sequence in which they were created.
- b. Forensic evidence on a smartphone or storage medium can also indicate who has used or controlled the smartphone or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the smartphone or storage medium at a relevant time.
- c. A person with appropriate familiarity with how a smartphone works can, after

examining this forensic evidence in its proper context, draw conclusions about how the smartphone was used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium, such as a smartphone, that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the smartphone and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
 - e. Further, in finding evidence of how a computer or other electronic device, such as a smartphone, was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) along with passwords, encryption keys and other access devices, may be relevant to establishing the user's intent.
3. In most cases, a thorough search of an Apple iPhone model A1586 with International Mobile Equipment Identity (IMEI) 356954068692712, and a Toshiba Satellite computer with serial number 1D227418Q, for information stored on storage media requires the seizure of the physical storage media and later off-site review consistent with the warrant. Seizure is necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:
- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer or smartphone has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
 - b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware

and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats and may require off-site reviewing with specialized forensic tools. Formats may include flash memory cards in various formats with the associated storage capabilities of the cellular device.
4. Your affiant also knows that electronic storage devices (like smartphones) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order and with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data store, and it would be generally impossible, due to the equipment needed and the time necessary to accomplish this kind of data search on site.
5. Your affiant is additionally aware that searching smartphones for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. Since cellular phone evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.
6. Based on your affiant's knowledge, training, and experience, your affiant knows that smart phone storage files or remnants of such files can be recovered months or even years after they have been downloaded onto the internal memory, deleted or viewed via the Internet. Even when files have been deleted, they can be recovered months or years later using forensics tools. This is so because when a person "deletes" a file on a cellular phone, the data contained in the file does not actually disappear; rather, that data remains on the internal memory until it is overwritten by new data.
7. Based on your affiant's knowledge, training, and experience, your affiant knows that smart phone are often used by those involved in access device fraud whether that be communicating with coconspirators, or using the device to access information that contains the stolen access device information.

WHEREFORE, I respectfully request that a warrant be issued authorizing Homeland Security Investigations, with appropriate assistance from other law enforcement officers, to forensically review the Apple iPhone model A1586 with International Mobile Equipment Identity (IMEI) 356954068692712, and a Toshiba Satellite computer with serial number 1D227418Q described in Attachment A and therein search for, seize, and examine the items set forth above and in Attachment B.

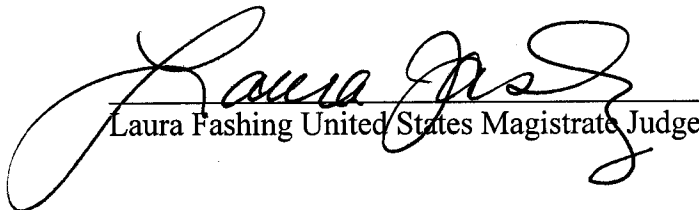
This affidavit was reviewed and approved by AUSA Jonathon Gerson.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge. FURTHER AFFIANT SAYETH NOT.



Ryan Palmiter, Special Agent
Homeland Security Investigations

Subscribed and sworn before me this 22nd day of August, 2016.



Laura Fashing United States Magistrate Judge

ATTACHMENT A
DESCRIPTION OF PROPERTY TO BE SEARCHED

The PROPERTY described as;

- A) Apple iPhone model A1586 with International Mobile Equipment Identity (IMEI)
356954068692712
- B) Toshiba Satellite computer with serial number 1D227418Q

These items are currently in the possession of The Albuquerque Police Department at The Forensic Science Center, 5350 2nd Street NW, Albuquerque, NM 87107.

ATTACHMENT B

Items to be searched, seized and analyzed include all evidence, fruits and instrumentalities pertaining to violations of Title 18, United States Code § 1028A – Aggravated Identity Theft and Title 18, United States Code § 1029 – Access Device Fraud, and contained within the devices listed in attachment A.

Records and electronically stored documents that show the communications concerning identity theft and/or fraud/misuse of visas permits and other documents; as well as evidence of Title 18, United States Code § 1029 – Access Device Fraud:

1. Computer hard drives, or other physical objects upon which computer data can be recorded that is called for by this warrant, or that might contain things otherwise called for by this warrant including:
 - a. Evidence of who used, owned, or controlled the items described in Attachment A at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence.
 - b. Evidence of software that would allow others to control the items described in Attachment A, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.
 - c. Evidence of the lack of such malicious software;
 - d. Evidence of the attachment of other storage devices or similar containers for electronic evidence.
 - e. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the items described in Attachment A.
 - f. Evidence of the times the items described in Attachment A was used.
 - g. Passwords, encryption keys, and other access devices that may be necessary to access the items described in Attachment A.
 - h. Contextual information necessary to understand the evidence described in this attachment.
 - i. Records of internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.
2. During the course of the search, photographs of the searched property may also be taken to record the condition thereof and/or the location of items therein.